Theory Meets Practice in the Algorand Blockchain

Victor Luchangco ✉
Algorand, Inc., Boston, MA, USA

Abstract

Robust and effective distributed systems require good theory and good engineering, not separately but in concert: user requirements and system constraints are not merely implementation details but often must inform the design of algorithms for such systems. Blockchains are an excellent example. The heart of a blockchain is its (Byzantine) consensus protocol, and consensus protocols have been extensively studied in the theory community for decades. But traditional consensus protocols are not directly applicable to blockchains, which have, or hope to have, millions of participants. Furthermore, public blockchains, which allow anyone to participate, must have some mechanism to guarantee the security of the protocol, and traditional fault models do not adequately capture the assumptions of such mechanisms. In this talk, I will discuss these and other ways in which theory and practice meet in the context of the Algorand blockchain, and how Algorand is able to achieve high transaction throughput with low latency.

2012 ACM Subject Classification Theory of computation → Distributed algorithms; Computer systems organization → Dependable and fault-tolerant systems and networks

Keywords and phrases Theory and practice, Design of distributed systems, Blockchain, Consensus, Algorand

Digital Object Identifier 10.4230/LIPIcs.OPODIS.2022.1

Category Invited Talk

© Victor Luchangco;
licensed under Creative Commons License CC-BY 4.0